Safeguarding PII

2010 DoD FOIA/Privacy Act Conference

Presented by

Samuel P. Jenkins, Director,

Defense Privacy and Civil Liberties Office

April 28, 2010

Safeguarding PII

Agenda:

- DoD 5400.11-R Appendix 1
- OMB M-07-16 Requirements
- June 5, 2009 Memorandum Requirements
- Privacy Impact Assessments (PIA)
- PIA/SORN Essential Elements Crosswalk

Safeguarding PII

DoD 5400.11-R Appendix 1

DoD 5400.11-R

Appendix 1 – Safeguarding PII

- Risk Management and Safeguarding Standards
- Minimum Administrative Safeguards
- Physical Safeguards

DoD 5400.11-R

Appendix 1 – Safeguarding PII (cont'd)

- Technical Safeguards
- Special Procedures
- Record Disposal

Safeguarding PII

OMB M-07-16 Requirements

Safeguarding PII

OMB M-07-16

- OMB M-07-16 implemented new PII safeguarding requirements.
- These requirements were implemented throughout DoD in the June 5, 2009 Memorandum “Safeguarding Against and Responding to the Breach of Personally Identifiable Information (PII)”.

Safeguarding PII

The OMB M-07-16 Requirements Are:

1. Safeguarding PII
2. Incident Reporting
3. External Breach Notification
4. Rules and Consequences

OMB M-07-16 Requirements

1. Safeguarding PII

A. Current Requirements

1. Privacy Act Requirements
    a. Establish Rules of Conduct
    b. Establish Safeguards
    c. Maintain accurate, relevant, timely, and complete information

OMB M-07-16 Requirements

1. Safeguarding PII (cont'd)

2. Security Requirements
   a. Assign an impact level to all information and information systems
   b. Implement minimum security requirements and controls
   c. Certify and accredit information systems
   d. Train employees

OMB M-07-16 Requirements

1. Safeguarding PII (cont'd)

B. Privacy Requirements

1. Review and Reduce the Volume of Personally Identifiable Information
    a. Review Current Holdings
2. Reduce the Use of Social Security Numbers
    a. Eliminate Unnecessary Use
    b. Explore Alternatives

OMB M-07-16 Requirements

1. Safeguarding PII (cont'd)

C. Security Requirements

- Encryption
- Control Remote Access
- Time-Out Function
- Log and Verify
- Ensure Understanding of Responsibilities

OMB M-07-16 Requirements

2. Incident Reporting

A. Existing Requirements
   1. FISMA Requirements
   2. Incident Handling and Response Mechanism

B. Modified Agency Reporting Requirements
   1. US-CERT Modification
   2. Develop and Publish a Routine Use
      a. Effective Response
      b. Disclosure of Information

OMB M-07-16 Requirements

3. External Breach Notification

A. Background

1. Harm
2. Requirement
3. Threshold Questions
4. Chilling Effects of Notices

OMB M-07-16 Requirements

3. External Breach Notification (cont'd)

B. New Requirement

1. Whether Breach Notification is Required
2. Timeliness of the Notification
3. Source of the Notification
4. Contents of the Notification

OMB M-07-16 Requirements

3. External Breach Notification (cont'd)

B. New Requirement

5. Means of Providing Notification
6. Who Receives Notification: Public Outreach in Response to a Breach

OMB M-07-16 Requirements

4. Rules and Consequences

A. New Requirement: Rules and Consequences Policy

1. Affected Individuals
2. Affected Actions
3. Consequences

Safeguarding PII

June 5, 2009 Memorandum Requirements

DoD Implementation Of OMB Requirements

The June 5, 2009 Requirements Are:

1. Definitions
2. Training
3. Review of PII Holdings
4. Incident Reporting and Handling Requirements

DoD Implementation Of OMB Requirements

Part I. Definitions – Current DoD Policy

A. Personally Identifiable Information (PII), as set forth in DoD Directive 5400.11, para E2.e and DoD 5400.11-R, para DL1.l4, is defined as follows:

- "Personal Information. Information about an individual that identifies, links, relates, or is unique to, or describes him or her, e.g., a Social Security Number; age; military rank; civilian grade; marital status; race; salary; home/office phone numbers; other demographic, biometric, personnel, medical, and financial information, etc. Such information is also known as personally identifiable information (i.e., information which can be used to distinguish or trace an individual's identity, such as their name, Social Security Number, date and place of birth, mother's maiden name, and biometric records, including any other personal information which is linked or linkable to a specified individual)."

DoD Implementation Of OMB Requirements

Part I. Definitions – Current DoD Policy (cont'd)

B. DoD 5400.11-R defines "lost, stolen or compromised information," otherwise termed a breach" as follows:

- "Actual or possible loss of control, unauthorized disclosure, or unauthorized access of personal information where persons other than authorized users gain access or potential access to such information for an other than authorized purposes where one or more individuals will be adversely affected. Such incidents also are known as breaches."

DoD Implementation Of OMB Requirements

Part I. Definitions – New DoD Policy

- "DoD Components are to utilize the factors outlined in Appendix A and Table 1, or other approved methodology, to make determinations of risk of harm associated with a breach (loss, theft or compromise) of PII."

DoD Implementation Of OMB Requirements

Appendix A – Identity Theft Risk Analysis

1. Nature of the Data Elements Breached
2. Number of Individuals Affected
3. Likelihood the Information is Accessible and Usable
4. Likelihood the Breach May Lead to Harm
   - Broad Reach of Potential Harm
   - Likelihood Harm Will Occur
5. Ability of the Agency to Mitigate the Risk of Harm

DoD Implementation Of OMB Requirements

Table 1. Risk Assessment Model

No.	Factor	Risk Determination	Low: Moderate: High:	Comments: All breaches of PII, whether actual or suspected, require notification to US-CERT Low and moderate risk/harm determinations and the decision whether notification of individuals is made, rest with the Head of the DoD Component where the breach occurred All determinations of high risk or harm require notifications
1.	What is the nature of the data elements breached? What PII was involved?			
	a. Name only	Low		Consideration needs to be given to unique names; those where one or only a few in the population may have or those that could readily identify an individual, i.e., public figure
	b. Name plus 1 or more personal identifier (not SSN, Medical or Financial)	Moderate		Additional identifiers include date and place of birth, mother's maiden name, biometric record and any other information that can be linked or is linkable to an individual
	c. SSN	High		
	d. Name plus SSN	High		
	e. Name plus Medical or Financial data	High		
2.	Number of Individuals Affected			The number of individuals involved is a determining factor in how notifications are made, not whether they are made

DoD Implementation Of OMB

3.	What is the likelihood the information is accessible and usable? What level of protection applied to this information?			
	a. Encryption (FIPS 140-2)	Low		
	b. Password	Moderate/High		Moderate/High determined in relationship to category of data in No. 1
	c. None	High		
4.	Likelihood the Breach May Lead to Harm	High/Moderate/Low		Determining likelihood depends on the manner of the breach and the type(s) of data involved
5.	Ability of the Agency to Mitigate the Risk of Harm			
	a. Loss	High		Evidence exists that PII has been lost; no longer under DoD control
	b. Theft	High		Evidence shows that PII has been stolen and could possibly be used to commit ID theft?
	c. Compromise			
	(1) Compromise w/I DoD control	Low High		No evidence of malicious intent Evidence or possibility of malicious intent
	(2) Compromise beyond DoD control	High		Possibility that PII could be used with malicious intent or to commit ID theft

DoD Components are to thoroughly document the circumstances of all breaches of PII and the decisions made relative to the factors above in reaching their decision to notify or not notify individuals.

DoD Implementation Of OMB Requirements

Part II. Training

A. New DoD policy shall be:

1) Training must be commensurate with an individual's responsibilities.
2) Training will be a prerequisite before permitted access to DoD systems.
3) Such training is now mandatory for affected DoD personnel and contractors.

DoD Implementation Of OMB Requirements

Part II. Training (cont'd)

B. To meet requirements, Components shall ensure receipt of Privacy Act training, as follows:

- Orientation Training
- Specialized Training
- Management Training
- Privacy Act Systems of Records Training

DoD Implementation Of OMB Requirements

Part II. Training (cont'd)

C. Annual Refresher Training

- Shall be provided to ensure employees and managers, as well as contractor personnel, continue to understand their responsibilities.
- All personnel with authorized access to PII shall annually sign a document clearly describing their responsibilities and acknowledging their understanding.

DoD Implementation Of OMB Requirements

Certification of Initial/Annual Refresher Training

The certification may read as follows:

"This is to certify that I have received initial/annual refresher training on my privacy and security responsibilities. I understand that I am responsible for safeguarding personally identifiable information that I may have access to incident to performing official duties. I also understand that I may be subject to disciplinary action for failure to properly safeguard personally identifiable information, for improperly using or disclosing such information, and for failure to report any known or suspected loss or the unauthorized disclosure of such information."

_____ (Signature)

_____ (Print Name)

_____ (Date)

_____ (DoD Component/Office)

DoD Implementation Of OMB Requirements

Part II. Training (cont'd)

D. DoD Components shall examine such training, and if not already included, shall expand their training materials and program to include specific privacy and security awareness segments to their privacy and security training program(s).

DoD Implementation Of OMB Requirements

Part III. Review of PII Holdings

- As part of this year's instructions for FISMA privacy reporting, DoD Components will be required to:
  - Confirm that they have established, or are in the process of establishing, PII review plans;
  - Provide a schedule by which they will periodically update their review of their holdings following the initial review.

DoD Implementation Of OMB Requirements

Part III. Review of PII Holdings (cont'd)

It shall be DoD policy that:

A. DITPR identifies all Components' automated systems containing PII.

B. Updates to OMB designed so that:

   1) IT systems with PII reviewed on same cycle as DIACAP.

   2) PIA SORNs reviewed *at least once* every two years.

C. Components shall report results to DPO on FISMA schedule.

DoD Implementation Of OMB Requirements

Part IV. Incident Reporting and Handling Requirements

A. Agency Reporting Requirements

B. External Breach Notification Requirements

C. Timeliness of the Notification

DoD Implementation Of OMB Requirements

Part IV. Incident Reporting and Handling Requirements (cont'd)

D. Source of the Notification

E. Contents of the Notification

F. Means of Providing Notification

G. Who Receives Notification

Safeguarding PII

Privacy Impact Assessments (PIA)

Safeguarding PII

Privacy Threshold Assessment (PTA)

- DHS uses Privacy Threshold Assessments (PTA) to determine if a PIA is necessary.
- DoD practice is to perform a PIA


Homeland Security

The Privacy Office
U.S. Department of Homeland Security
Washington, DC 20528
703-235-0780, pia@dhs.gov
www.dhs.gov/privacy

Privacy Threshold Analysis
Version date: June 10th, 2009
Page 1 of 6

PRIVACY THRESHOLD ANALYSIS (PTA)

This form is used to determine whether
a Privacy Impact Assessment is required.

Safeguarding PII

What is a PIA?

A "*Privacy Impact Assessment (PIA)*--is an analysis of how information is handled:

- to ensure handling conforms to applicable legal, regulatory, and policy requirements regarding privacy,
- to determine the risks and effects of collecting, maintaining and disseminating information in identifiable form in an electronic information system, and
- to examine and evaluate protections and alternative processes for handling information to mitigate potential privacy risks."

OMB 03-22 (9/26/2003), EGOV 208(b)

Safeguarding PII

When is a PIA Required?

- **When PII is collected, a PIA is required for**:
  - Existing information systems and electronic collections where a PIA has not previously been completed to include systems that collect PII about Federal personnel and contractors.
  - New information systems or electronic collections:
    - Prior to developing or purchasing, and
    - when converting paper-based records to electronic systems.

Safeguarding PII

When is a PIA not Required?

- When the information system or electronic collection:
  - Does not collect, maintain or disseminate personal identifying information
  - Is a National Security System (including systems that process classified information)

Safeguarding PII

PIA/SORN Essential Elements Crosswalk

Safeguarding PII

Privacy Impact Assessment (PIA)/ System of Record Notice (SORN) Essential Elements Crosswalk	
PIA	**SORN**
What privacy information is collected	Categories of Records in the System
Why the information is collected	Authority/Purpose(s)
What the intended uses are for the information	Purposes(s)
With whom the information is shared	Routine Uses
What opportunities individuals have to decline to provide PII	Privacy Act Statement/Notification procedure
How information is secured	Safeguards
What privacy risks need to be addressed	Narrative Statement/Probable or potential effects on the privacy of individuals.
Whether a System of Records Notice (SORN) exists	(Not applicable)

Safeguarding PII

Privacy Impact Assessment (PIA)/ System of Record Notice (SORN) Essential Elements Crosswalk	
PIA	**SORN**
What privacy information is collected? • Nature of the information • Scope of the information	Categories of Records in the System • Describe the types of individually identifiable information maintained in the system, e.g., social security number, date of birth, patient medical history, school applications

Safeguarding PII

Privacy Impact Assessment (PIA)/ System of Record Notice (SORN) Essential Elements Crosswalk	
PIA	**SORN**
Why is the information collected? • Describe the purpose of the collection, e.g., verification, identification, authentication, data matching	Authority • Describe the specific legal authority (citation and descriptive title) for maintenance of the system. Only a statute or Executive Order of the President may be cited.

Safeguarding PII

Privacy Impact Assessment (PIA)/ System of Record Notice (SORN) Essential Elements Crosswalk	
PIA	**SORN**
What are the intended uses for the information? • How will the information be used to fulfill the purpose previously stated?	Purpose(s) • Describe the purpose for which the system of records was established and uses of the information internal to the organization.

Safeguarding PII

Privacy Impact Assessment (PIA)/ System of Record Notice (SORN) Essential Elements Crosswalk	
PIA	**SORN**

With whom is the information shared?
 	
• Within the Agency
 	
• With another Federal Agency
 	
• State or local agency
 	
• Contractor(s)
	Routine Uses
	
	• Describe routine uses of the information outside the organization which are authorized for records in the system. Each individual routine use should identify
	  • the third party to whom disclosure is authorized,
	  • the type of information to be disclosed and
	  • the purpose of the disclosure

Safeguarding PII

Privacy Impact Assessment (PIA)/ System of Record Notice (SORN) Essential Elements Crosswalk	
PIA	**SORN**
What opportunities will individuals have to decline to provide PII? • Is this collection statutorily mandated? • If voluntary, how can individuals grant or withhold consent?	Privacy Act Statement/Notification procedure • Does the Privacy Act Statement accurately reflect the essential elements of the data collection? • Provide the title and office to which the individual would write to determine whether or not the system contains a record about the individual, how they access their record, and what information the individual needs to provide to verify their identity.

Safeguarding PII

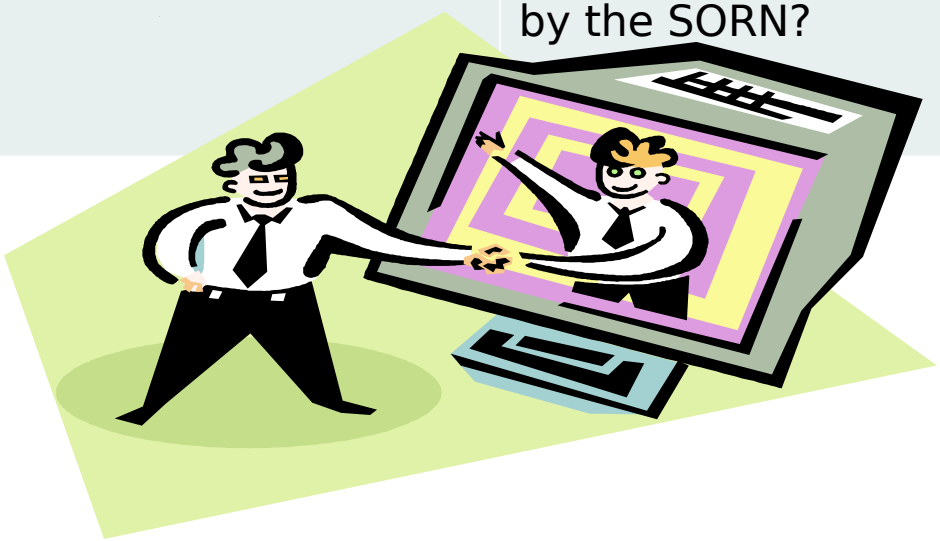
Privacy Impact Assessment (PIA)/ System of Record Notice (SORN) Essential Elements Crosswalk	
PIA	**SORN**
How is information secured? • Physical Controls, e.g., security guards, locks, closed circuit TV, safe • Technical Controls, e.g., firewall, public key infrastructure (PKI) Certificates, encryption, biometrics • Administrative Controls, e.g., backups, periodic security audits, methods to ensure only authorized persons access PII	Safeguards • Describe all measures in place to minimize the risk of unauthorized access to or disclosure of records in the system. Identify the categories of employees who are authorized to have access to the records.

Safeguarding PII

Privacy Impact Assessment (PIA)/ System of Record Notice (SORN) Essential Elements Crosswalk	
PIA	**SORN**
What privacy risks need to be addressed? • How do information handling practices at each stage of the "information life cycle" (i.e., collection, use, retention, processing, disclosure and destruction) affect individuals'' privacy? • For existing information systems or electronic collections, what measures have been put in place to address identified privacy risks? • For new information systems or collections, what measures are planned for implementation to address identified privacy risks?	Narrative Statement/Probable or potential effects on the privacy of individuals. • What is/could be the impact on the individual as a result of this compilation of information? • What impact would a breach of this information have on the individual?

Safeguarding PII

Privacy Impact Assessment (PIA)/ System of Record Notice (SORN) Essential Elements Crosswalk	
PIA	**SORN**
Does a SORN exist to correspond with the collection documented in the PIA?	Does/Do PIA(s) exist to correspond with the data collection represented by the SORN?



Safeguarding PII

PRIVAC
ASSESSMENT (PIA)

DoD Information System/Electronic Collection Name:

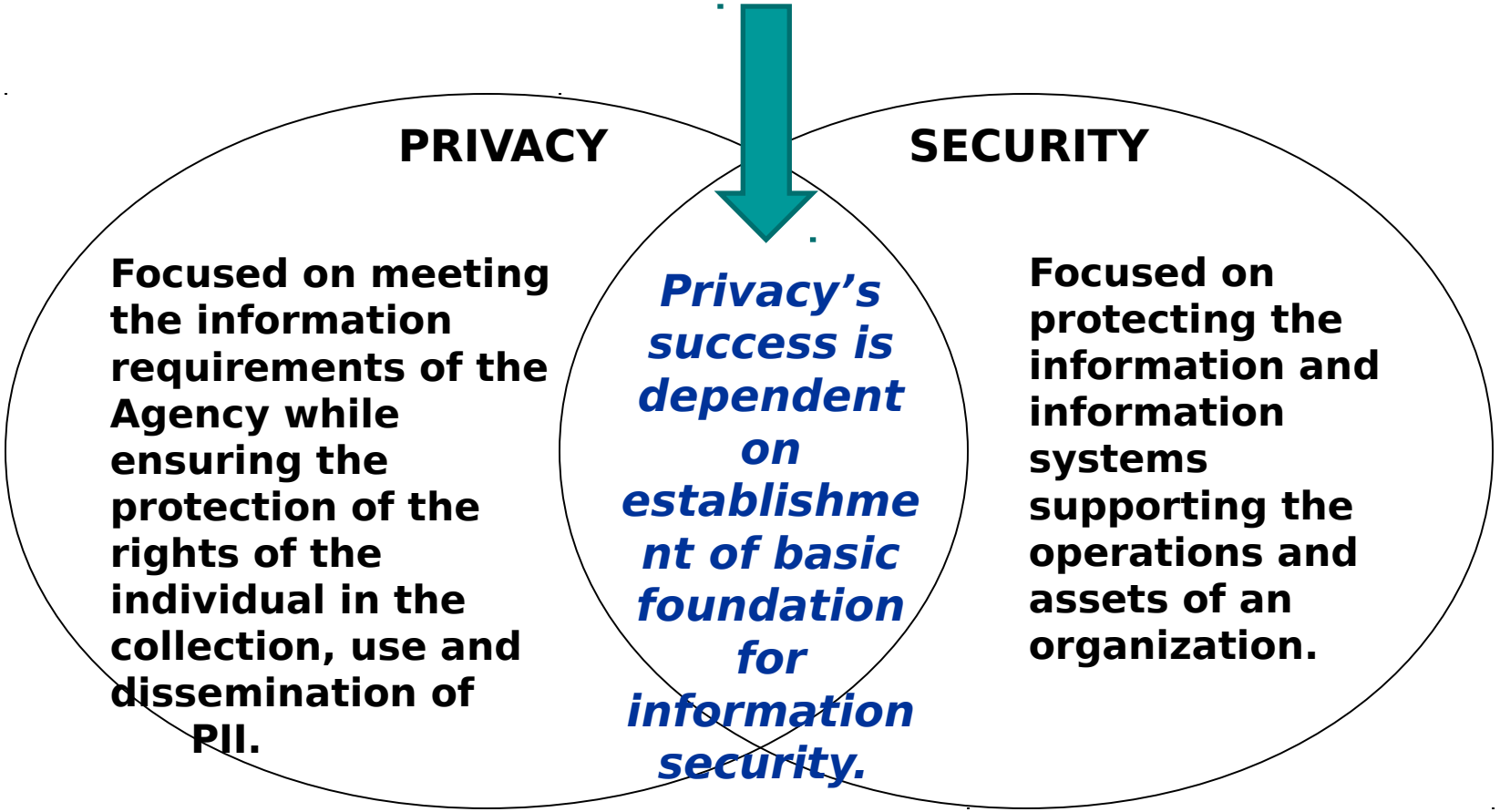
DoD Component Name:

SECTION 4: REVIEW AND APPROVAL SIGNATURES Prior to the submission of the PIA for review and approval, the PIA must be coordinated by the Program Manager or designee through the Information Assurance Manager and Privacy Representative at the local level.	
Program Manager or Other Official Signature (to be used at Component discretion)	
Component Senior Information Assurance Officer Signature or Designee	
Component Privacy Officer Signature	
Component CIO Signature (Reviewing Official)	

Source: DD Form 2930

Safeguarding PII

Critical Privacy – Security Interfac



NIST Draft Guide to Protecting the Confidentiality of (PII) (1/09)

Questions?